Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

December 7, 2021

Challenge yourself with our NEW Gift Card Scam Awareness quiz!

This week's stories:

Canadian energy, health, manufacturing sectors were major targets of ransomware attacks: cyber spy agency

More than half of the known ransomware victims in Canada this year were critical infrastructure providers, according to a new threat assessment from Canada's cyber spies, and the number is likely even higher.

As part of a push a new awareness campaign, the Communications Security Establishment (CSE), Canada's foreign signals intelligence agency, released a ransomware bulletin Monday looking at the key trends of ransomware in 2021.

https://www.cbc.ca/news/politics/ransomware-critical-infrastructure-cse-1.6274982

Click above link to read more.

Back to top

Canadian health, energy sectors increasingly targeted by ransomware attacks

Canada's cyber defence agency says more than half of Canadian ransomware victims in 2021 were in critical sectors like health care, energy and manufacturing.

Now, the Communications Security Establishment (CSE) and the RCMP are urging Canadian businesses to upgrade their cyber security — and to report any ransomware attacks, even if they decide to pay the hackers.

https://globalnews.ca/news/8427930/canadian-health-energy-sectors-increasingly-targeted-by-ransomware-attacks/

Click above link to read more.

Back to top

Rideau Hall internal cyber network hit by 'breach' — effects unclear

Rideau Hall confirms there has been a "breach" of the internal networks at the office that supports the work of the governor general — but the potential impact is so far unclear.

In a statement issued Thursday morning, the Office of the Secretary to the Governor General said there had been "an unauthorized access to its internal network."

https://globalnews.ca/news/8419717/rideau-hall-cyber-incident-2021/

Click above link to read more.

Back to top

Take steps to fend off ransomware attacks, federal ministers urge Canadians

Citing a dramatic increase in ransomware attacks, several federal ministers are urging Canadians to bolster their cybersecurity practices.

In an open letter today, the ministers encourage organizations to adopt the latest security measures, build a response plan and ensure information technology staff are well-prepared to respond to incidents.

https://www.ctvnews.ca/politics/take-steps-to-fend-off-ransomware-attacks-federal-ministers-urge-canadians-1.5695256

Click above link to read more.

Back to top

Ransomware attacks hit French-public school board

An October 18 ransomware attack has left personal data exposed by the local French-Public school board.

The Conseil des écoles publiques de l'Est de l'Ontario issued a press release November 30 announcing it had been attacked, and that after resecuring the network it was discovered that some files stored at its board office had been stolen and held for ransom.

https://www.thestar.com/news/canada/2021/12/02/ransomware-attack-hits-french-public-school-board.html

Click above link to read more.

Back to top

---

5 Ways to Keep Fraudsters at Bay Over the Holidays

As we near the end of the calendar year, many of us may be looking forward to some time off with friends and family and a fresh start in the new year. In the retail, e-commerce, and financial sectors, however, the end of the year brings the holiday shopping season. This is the busiest and most critical time of the year for those types of businesses.

Simply put, there is a lot of money at stake during this peak shopping season. Not surprisingly, attackers and fraudsters are keenly aware of this. They hone their skills and target their efforts to maximize their financial gain by maximizing customer losses.

https://www.darkreading.com/edge-articles/5-ways-to-keep-fraudsters-at-bay-over-the-holidays

Click above link to read more.

Back to top

How IT pros can better track and report cybersecurity KPIs

More than ever, provider and payer organizations understand the value of analytics and data visualization, and have become adept at tracking and reporting a galaxy of metrics and key performance indicators to monitor their clinical, financial and operational well-being.

It's equally important when running and adapting effective cybersecurity programs, as Omar Khawaja, chief information security officer of Highmark Health, will explain next week at the HIMSS Healthcare Cybersecurity Forum.

https://www.healthcareitnews.com/news/how-it-pros-can-better-track-and-report-cybersecurity-kpis

Click above link to read more.

Back to top

USB Devices the Common Denominator in All Attacks on Air-Gapped Systems

Cyberattacks on air gapped systems, including the sophisticated and dangerous 2010 Stuxnet attack that crippled a uranium enrichment facility, all have one thing in common: a USB stick.

A new ESET study of 17 malware frameworks that threat actors have used over the past decade to target air-gapped systems showed every one of them used a USB drive to introduce malware into the environment and extract data from there. The security vendor found that the best defense for organizations against attacks on air-gapped systems is to restrict USB use as much as possible and to monitor them closely in situations where the devices need to be used.

https://www.darkreading.com/attacks-breaches/usb-devices-common-denominator-in-all-attacks-on-air-gapped-systemsd

Click above link to read more.

Back to top

AI in Cybersecurity: How to Cut Through the Overhype and Maximize the Potential

Artificial intelligence (AI), machine learning (ML), and deep learning (DL) are often applied in cybersecurity, but their applications may not always work as intended. ISACA's new publication, AI Uses in Blue Team Security, looks at AI, ML and DL applications in cybersecurity to determine what is working, what is not, what looks encouraging for the future and what may be more hype than substance.

Leveraging interviews with some of the engineers behind these technologies, firsthand examination and use of some of the related products, and observations of chief information security officers (CISOs) and chief information officers (CIOs), *AI Uses in Blue Team Security* seeks to determine whether marketing tactics obscure reality when it comes to new security technology.

https://www.businesswire.com/news/home/20211202005861/en/AI-in-Cybersecurity-How-to-Cut-Through-the-Overhype-and-Maximize-the-Potential

Click above link to read more.

Back to top

Report finds 'glaring gaps' in financial sector's cybersecurity measures

The rapid pace of digital transformation brought about by the COVID-19 pandemic has left glaring gaps in the financial services sector's cybersecurity measures, putting many businesses at heightened risk of ransomware attacks – an issue that could take at least two years to close, a new study has revealed.

Global data management giant Veritas Technologies surveyed 2,050 information technology executives from 19 countries, including 245 respondents from the financial services sector, and found that companies in the industry were struggling to keep pace in terms of cyber protection compared to those from other sectors.

https://www.insurancebusinessmag.com/uk/news/cyber/report-finds-glaring-gaps-in-financial-sectors-cybersecurity-measures-318433.aspx

Click above link to read more.

Back to top

BitMart: Crypto-exchange loses $150m to hackers

Crypto-currency exchange BitMart says hackers have stolen about $150m (£113m) worth of tokens from its "hot wallets".

Those affected, one storing Ethereum and one Binance Smart Chain tokens, "carry a small percentage of assets on BitMart and all of our other wallets are secure and unharmed", it said.

https://www.bbc.com/news/technology-59549606

Click above link to read more.

Back to top

Spar cyber attack hits more than 300 convenience stores

A cyber attack has hit more than 300 Spar convenience stores across the north of England with some forced to close their doors.

The attack on Sunday targeted James Hall & Company in Preston, Lancashire, which operates Spar's tills and IT systems.

https://www.bbc.com/news/uk-england-lancashire-59554433

Click above link to read more.

Back to top

30% security breaches caused by weak passwords: GoodFirms 2021 Research

GoodFirms, the leading research, listing, and review platform, recently published its latest survey report- Top Password Strengths and Vulnerabilities: Threats, Preventive Measures, and Recoveries. This survey from GoodFirms outlines the current password behavior of online users, risk factors associated with password management, and the best measures, policies, and practices to safeguard passwords from attacks or breaches. 30% of surveyees reported password leaks and security breaches owing to poor password practices and weak password setups.

The research highlights a few common insecure password practices of users, such as sharing passwords with colleagues, family members, and friends; jotting down passwords on sticky notes, papers, planners, changing passwords only when prompted; or using the same passwords for multiple sites.

https://www.prnewswire.com/news-releases/30-security-breaches-caused-by-weak-passwords-goodfirms-2021-research-301438687.html

Click above link to read more.

Back to top

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

For previous issues of Security News Digest, visit the current month archive page at:

http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

To learn more about information security issues and best practices, visit us at:

https://www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer